SYNGRESS

SECURING VoIP

Keeping Your VoIP Network Safe

Regis (Bud) Bates

Securing VoIP

Keeping Your VoIP Network Safe

Page left intentionally blank

Securing VoIP

Keeping Your VoIP Network Safe

Regis J. (Bud) Bates

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an Imprint of Elsevier

SYNGRESS

Acquiring Editor: Steve Elliot
Editorial Project Manager: Benjamin Rearick
Project Manager: Paul Prasad Chandramohan
Designer: Greg Harris

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Copyright © 2015 Elsevier Inc. All rights reserved

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-417039-1

For information on all Syngress publications
visit our website at http://store.elsevier.com/

Contents

Technical editor biography

Tom Ring is currently employed by IQ Services, a Minneapolis-based company that provides performance load testing and availability monitoring services for Fortune 500 contact centers. He holds a dual position at the firm, serving both as the Lead Sales Engineer and as its Security Manager.

Mr. Ring has been employed in the telecommunications industry for over 30 years. His positions have included: Senior Systems Administrator at Pixius Communications, Support Engineer at Harmonic Systems, Level 3 Engineer/Programmer at Norstan Communications, Field Support Engineer at Ericsson Development, and National MD110 Field Engineer for Honeywell Communications Services Division.

While he rarely takes his Engineer's cap off, Ring enjoys amateur radio and autocross in his spare time. His favorite passion is maintaining his 1985 VW Westfalia Camper.

Favorite flavor – capsaicin.

Page left intentionally blank

About the author

Regis J. "Bud" Bates has more than 48 years of experience in telecommunications and information services and has long been considered a technology "Guru." He currently contributes to these fields as an author, consultant, expert witness, speaker, course developer, and teacher. He has written numerous books on the technologies.

With clients spanning the range of Fortune 100–500 companies, Mr. Bates has been involved in the design of major voice and data networks. His innovative ideas in implementation have been written up in trade journals and magazines. Many of his projects deal with multiple sites and countries using various architectures. A significant amount of Mr. Bates' work has also been in the wireless communications area. In his work with venture capitalists, he has consistently been on the mark with his projections for various analyses and studies.

Mr. Bates is known for his dynamic keynote speaking. With a style that is powerpacked and a delivery that is exciting, he knows how to captivate, engage, and motivate his audience. He motivates the sales force, customers, management team, and capital investors trying to figure out where the technology is heading for the future and where to invest. Regis Bates also develops and conducts various public and in-house seminars ranging from a managerial overview to very technical hands-on classes on Voice over IP, VoIP security, Wi-Fi networking, WIMAX networking, MPLS, DWDM, and IPv6. In the recent past he has focused much of his development and training activities on the convergence of three key areas: VoIP, security, and Wi-Fi.

He developed much on the wireless curriculum including Wi-Fi mesh, RF design, and Wi-Fi hands-on classes. He is very familiar with the Cisco routing and switching products, security products, and wireless products. He has served as an SME for many other training and development projects in the past.

As an independent consultant, Mr. Bates regularly lends his expertise to third-party assessment companies in the analysis, review, and recommendation of technology patents. In particular, Mr. Bates has assessed several portfolios from several large telecommunications and information system vendors, rank ordered the patents and technologies on a technical superiority basis, and monetized many of the portfolios so that his clients could acquire a reasonable portfolio for a reasonable price.

EXPERTISE

- Convergence technologies
- LAN, WAN, Ethernet, MPLS, ATM, frame relay, switching and routing
- Optical networks

- CATV networks
- TCP/IP
- Telephone equipment or operations
- Voice over the Internet Protocol (VoIP)
- Voice over Wi-Fi
- Wireless networks and technologies (cellular, GSM, CDMA/WCDMA, 3/4G GPRS, and SMS/IMS/MMS)
- Wired networks (PBX, voice, data, VoIP, 800 services)
- Disaster recovery/business continuity planning

PUBLICATIONS

Bates' books and seminars have been used by more than 166 colleges and universities around the globe, and Mr. Bates teaches many communications/computer courses and seminars in over a dozen countries globally.

BOOKS

1. Principles of Voice and Data. McGraw-Hill Educational Group, 2006
2. Voice and Data Communications Handbook, fifth ed. McGraw-Hill, 2006
3. Co-author on Wireless Networks Dictionary. Althos Publishing, 2006
4. cdmaOne and cdma2000. McGraw-Hill, 2003
5. General Packet Radio Services (GPRS). McGraw-Hill, 2002
6. Broadband Telecommunications Handbook, second ed. McGraw-Hill, 2002
7. Voice and Data Communications Handbook, fourth ed. McGraw-Hill, 2001
8. Optical Networking and Switching. McGraw-Hill, 2001
9. Voice and Data Communications Handbook, third ed. McGraw-Hill, 2000
10. Wireless Broadband Communications. McGraw-Hill, 2000
11. Nortel Networks Layer 3 Switching Handbook. McGraw-Hill, 2000
12. Broadband Telecommunications Handbook. McGraw-Hill, 1999
13. Client Server Internetworking. McGraw-Hill, 1998
14. Voice and Data Communications Handbook, signature ed. McGraw-Hill, 1998
15. Voice and Data Communications Handbook, first ed. McGraw-Hill, 1996
16. Wireless Networked Communications. McGraw-Hill, 1994
17. Disaster Recovery for LANs. McGraw-Hill, 1994
18. Introduction to T1/T3 Networking. Artech Publishing, 1992
19. Disaster Recovery for Telecommunications, Data and Networks. McGraw-Hill, 1991
20. Securing VoIP. Syngress, in press

ARTICLES

Mr. Bates has written several articles for different magazines over the years extolling the benefits of convergence, movement of information across broadband networking strategies, and user-oriented how-to documents:

1. IPTV Magazine Home PowerLine Networks, May 2006
2. IPTV Magazine Wireless Premises Distribution Networks, March 2006
3. IPTV Magazine Cable Premises Distribution Networks for IPTV, January 2006
4. CIO Magazine Pundit "Wireless Carriers Have the Goods," 2002
5. CIO Magazine Pundit "The Fiber Glut Myth," 2002
6. CIO Magazine Pundit "Cable vs DSL," 2002
7. Crisis Magazine "Disaster Recovery Planning," 1998
8. International Journal of Management "Managing Telecommunications," 1997
9. Disaster Recovery Magazine "Planning for Telecommunications Disasters," 1997

Page left intentionally blank

Acknowledgments

This book is designed to make you aware of the threats to Voice over IP (VoIP) on your wired network, introduce you to some of the issues that have already arisen, and guide you through an audit of where your network is exposed. Then, we will give you some ideas on integrating your IT security plan with your VoIP plan, preventing wherever possible the risks of eavesdropping and replay. Next, we will look at the wireless side of the VoIP networks that pose even greater risks. I hope you enjoy it for what it is, an overview to get you started.

This is not my first published book but it is my first with Elsevier. I once worked with the publisher, Steve Elliot, at another publisher and had lost track of Steve. It was he who found me again and convinced me to write this book. So I thank him for his perseverance in prodding me along the way. I also appreciate Steve's patience in my delays due to work schedules.

I would like to acknowledge Ben Rearick, Editorial Project Manager also at Elsevier Publishing, for his patient mannerism and encouraging attitude. Ben was responsible to keep me on track, a job that no one should be tagged with due to my fluctuating schedule. But through Ben's active role of keeping after me and prodding me to continue, we finally got the book completed.

I further want to acknowledge and thank my technical editor, Tom Ring. Tom had to keep me straight and offer his guidance in steering some of the content. He is an active VoIP'er so his input was invaluable. I look forward to working with him again someday.

I would be remiss if I did not acknowledge Gabriele, my wife, for her help in getting the graphics together. She was instrumental in taking an idea and rough drawing and creating a graphic that works for this book. Gabriele also made sure that I stayed on track as much as she could. It was her endless encouragement that led me to making the time to complete this work.

Finally there are a lot of people in the background, too many to mention. These are the production staff at Elsevier and the proofreaders. Moreover, the numerous vendors who welcomed me into their Partner programs and shared information with me freely are some of the unsung heroes here. They know who they are and I thank them for all their time and efforts.

Lastly, let me thank you, the reader, for two things. First, thanks for buying and reading this book. Second, thanks for being a part of this industry and helping it grow and mature. No book can solve every problem; no author can satisfy every reader's needs. Jointly, we all work together to improve the industry and help to make it what it is. You deserve the applause for all you do.

Thanks to you all!

Page left intentionally blank

CHAPTER

Introduction 1

CHAPTER OUTLINE

SECURING VOICE OVER INTERNET PROTOCOL (VoIP): KEEPING YOUR NETWORK SAFE

This book is intended as a primer for various organizations and individuals who may be planning to roll out a VoIP system. Generally speaking, if you have not experimented with VoIP in the past, a lot of new issues may surface that had not been considered in the older days of telephony. This book is structured in such a way as to handle those issues. In this chapter the following issues will be addressed:

1. History of telephony and why it was always considered to be safe
2. History of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and why it was always considered unsafe
3. The convergence of voice with data networks, and introduction to VoIP

4. Ingrained weaknesses in the deployment of a VoIP system including:
   a. Technological weaknesses
   b. Policy weaknesses
5. Statements of what is at risk when you deploy VoIP
6. Some of the threats that are known problems
7. Toll fraud
8. Theft of services
9. Loss of confidentiality
10. Eavesdropping
11. Hijacking
12. Voice mail hacking
13. Infrastructure attacks
14. Man-in-the-middle (MITM) attacks
15. Disruption or denial-of-service (DoS) attacks

As the reader might see, the issues can be many, yet they are not insurmountable. For example, when looking at the list overall, there are some pieces that can be considered and can be shorn up together. Actually, it is best if the security policies and procedures that organizations adopt and implement fully complement each other. Moreover, when dealing with VoIP, it is imperative that the security policies and procedures match those of the organization's information technology (IT) security, audit, and business resumption plans and they all coalesce as a single document. In fact, the closer the ties built in to blend the security, the better the installed system should work as a homogenous plan.

HISTORY OF TELEPHONY

In the very beginning of the voice telephony networks, the systems and services were always considered safe. The reason for this stems from the "Bell Telephone Company" philosophy. The Bell companies always ran a telephone wire from the Central Office (CO) to the customer's location. Different ways were used but for this discussion, the telephone wires were dedicated wires that ran from the CO along a wiring telephone pole line route to the end user's location (i.e., residence, business, etc.). In Figure 1.1 is shown a markup of how the wires were run from the CO to the end user over a pole line route. Because these bundles of wires were large, it was difficult for anyone to break into a pole line route or a buried route of 600–1200 pairs of wires and tap into them. It was possible but less than practical to break into such a link. Note that at the end user's location a single pair of wires was run into the customer location and a telephone set (typically an analog phone) was terminated on the wires.

Alternatively the dedicated wires were bundled together in a conduit or buried directly in the ground. For efficiency sake, the telephone wires were bundled in 600 or 1200 pairs of unshielded twisted pairs. As the larger bundles of wires were run closer to the customer site, they were split off at manholes or handholes where the pairs ultimately got separated to bring one to four pairs to the door. Shown in Figure 1.2 is the pole line and conduit combination.

FIGURE 1.1

The telephone company wires were run on a pole line route.

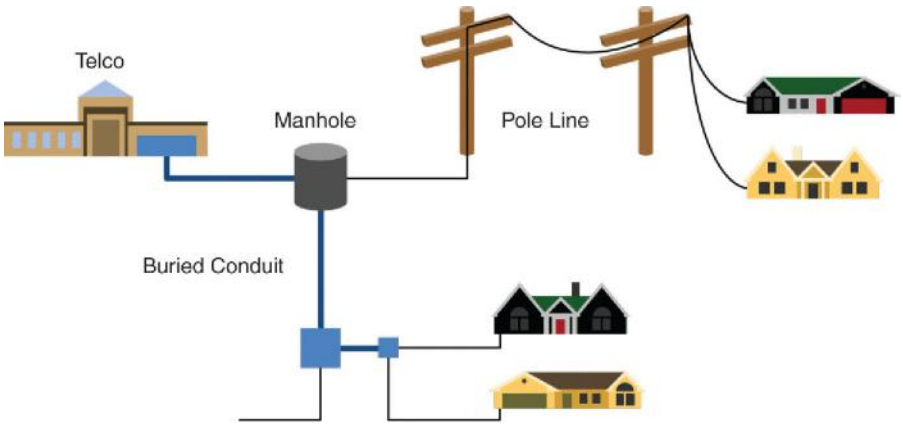

FIGURE 1.2

A mix of buried conduit and pole line route can also be used.

Throughout history, the telephone company CO has always been kept under lock and key. No outside personnel were allowed into the CO. The reason is obvious; the Bell Telephone Company was a natural monopoly and had total control over their wires. Entering the customer's site was a two- or four-pair cable as might be seen in Figure 1.3. This graphic shows a four-pair connection that is typically color coded so

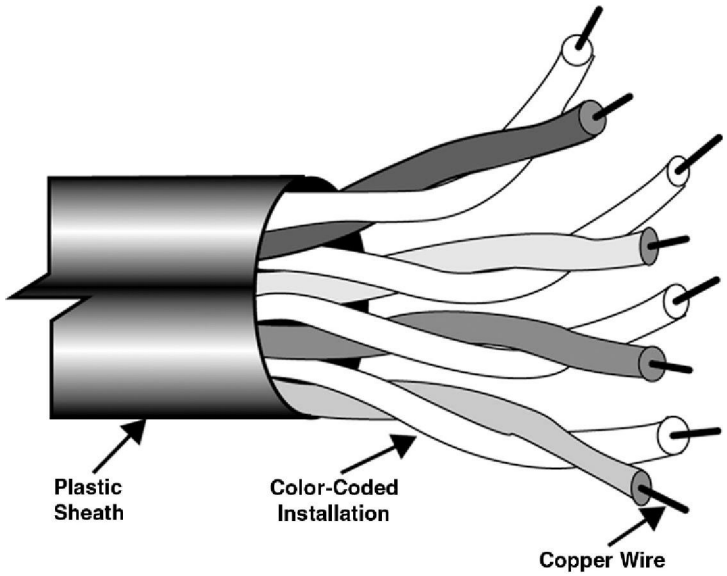

FIGURE 1.3

A four-pair wire was terminated at the customer location.

that dial tone can be brought to the end user. Under normal circumstances, the wires were thought to be dedicated from the CO to the telephone set.

Quite frankly, it was difficult for anyone other than a telephone company employee to figure out how the wiring was connected and how it worked, along the route. Thus, the cabling was considered safe. This is even truer when the cables were buried under the ground in a conduit. It took special knowledge to understand the myriad wires and the color schemes as well as the labeling.

For these reasons of complexity, visibility, and color code combinations, the telephone wires were always considered safe. Moreover, the architecture of the telephone network lent itself to security as the COs were not visibly labeled, there were little (or no) windows in the central switching offices, and the buildings required a user password or a card key system to get in. This kept the infrastructure fairly secure. Rather than belabor this thought, there have been breaches but they have been few and not highly publicized.

HISTORY OF THE INTERNET PROTOCOL

Without a doubt, much has happened since the inception of the Internet in the late 1960s. To be sure, the Internet was always considered an open access network. The intent was that colleges, universities, government agencies, and certain large corporations would use the Internet to share information. Thus, it had little security placed on it in the beginning. The entire purpose was for users to openly access data, files, and text messages (mail) that could be transferred between and among computers.

To facilitate this sharing a set of protocols was developed called TCP/IP. This protocol set was referred to as the DoD model in the beginning as the Internet was actually designed for the DoD under the auspices of the Defense Advanced Research Project Agency (DARPA) budgets for just this sharing of data.

Because DARPA needed the openness to share the files among many different computer systems, the protocols developed were open (no real security). As long as you knew how to connect, the access was wide open. Later, after several iterations, the need for securing the TCP/IP suite became rather obvious. Therefore, the TCP/IP in use today (still mostly IPv4), which was developed for use in 1983–1984, has been fixed like a patchwork quilt. New features were added, new security tools were added, and other tools were developed. Whereas the network was used primarily for the DoD use, it took a long time in coming. Yet in 1991 depending on how you view the evolution, the Internet became a public network to serve as the "information highway" of the future. It was then that the use and the exposure of the Internet exploded to a worldwide network accessible to all. The beginning network used a model of switches and routers that were different than the telephone companies. In fact, where the circuit-switched telephone network was used for voice and dial-up data, the Internet was based on a packet-switching network using TCP/IP. Figure 1.4 shows a mapping of the TCP/IP stack; although there are many different ways to show this stack, it is fairly easy to display many of the protocols in this one figure. As can be seen there are basically four different layers in this model. The bottom two layers include the hardware interfaces (looking at many different LAN and WAN connections) and the networking layer Internet Protocol (IP). At the transport layer Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are shown. These two different protocols are different to each other in terms of their function. Where TCP guarantees delivery, UDP does not guarantee delivery. It can be that VoIP runs on a TCP connection or a UDP connection. More will follow on that later. At the application layer in the TCP/IP stack as it was developed there are many applications that are supported. It was later that at the application layer new protocols were added to TCP/IP to support the VoIP services.

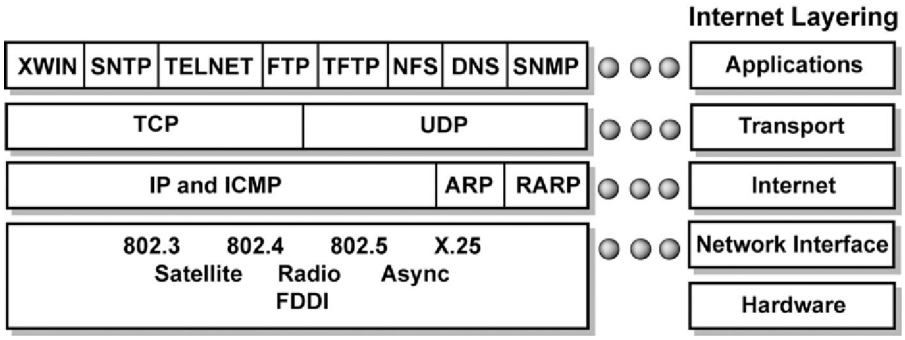

FIGURE 1.4

The TCP/IP stack as it existed early on.

After several years, breaches occurred across the Internet. As a result, a series of add-on features were created to patch the problems. These fixes included firewalls, new routers, more protocols to create a secure(r) environment, etc. It was these patches and fixes that helped create the Internet the way we know it today. Yet, some of the fixes got in the way of developments (i.e., in VoIP) that created the need for a workaround. Regardless of the issue, the protocols needed to be created to simplify and shore up the network, but the "evildoers" across the globe sought out many of the loopholes in the protocols and began exploiting them. Many of these exploits will be discussed later in this chapter and throughout others.

It was only a matter of time that voice and data convergence would rise to the forefront of the industry. Early on there were two separate directions that led the way for voice and data communications: the first was the voice telecommunications departments that often worked for finance or administration in corporate America. As such circuit-switched voice was the primary goal to satisfy the needs of the organization. The voice networks were deployed for daytime use (primarily) and the circuits sat idle off-hours. Consequently, the MIS[1] departments saw an opportunity to get a free ride for the data transmissions after hours by using both dedicated (leased) lines and circuit-switched lines. Second, after enough haggling and arguing, data transmission volumes began to overtake the voice traffic and newer methods of shipping data across the organization were needed. Packet switching was one of the methods. X.25 protocols were developed to handle reliable data transfer (guaranteed delivery and low error rates). However, this reliability came with a price. The costs were high and the delays encountered from retransmissions were high. Thus, a new method had to be found.

WHAT GOES AROUND COMES AROUND

As mentioned above, the Internet was developed for open communications between and among computer systems of different organizations. However, the original Internet protocols (such as IP) did not guarantee delivery, did not sequence the data properly, and did not provide error-free traffic. Consequently, the X.25 protocol was developed and rolled out as the salvation (1976) and went through several iterations of improvement. The X.25 network as shown in Figure 1.5 was primarily set up for dedicated access but was later used as a dial-up connection for smaller sites.

X.25 operates at layer 3 of the Open Systems Interconnection (OSI) model as seen in Figure 1.6. With that there was considerable overhead associated with transmitting data. Remarkably, the X.25 networks served the purpose for less than 20 years, which in the telecommunications networking environment was very short-lived.[2] One of the drawbacks of X.25 was slow speed, that being 56 or 64 kbps. The IT departments were fast approaching critical mass with the transmission of

[1]As it was called in the earlier days, management information system has gone through several iterations of naming until it became what is known today as the IT departments.
[2]X.25 was continued in use for certain organizations for years after this discussion but the masses began moving away from it earlier.

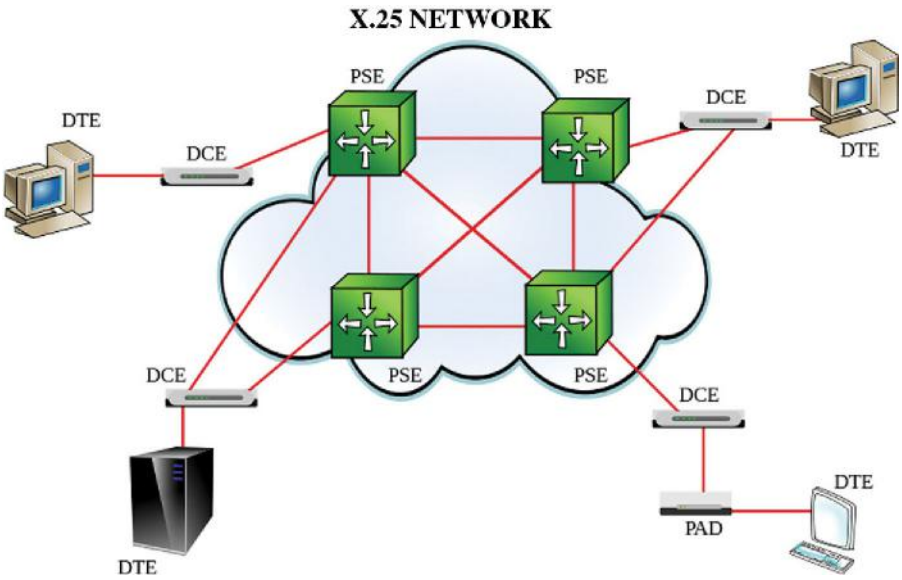

FIGURE 1.5

The X.25 network as it evolved.

FIGURE 1.6

X.25 operated at layer 3 of the OSI model.

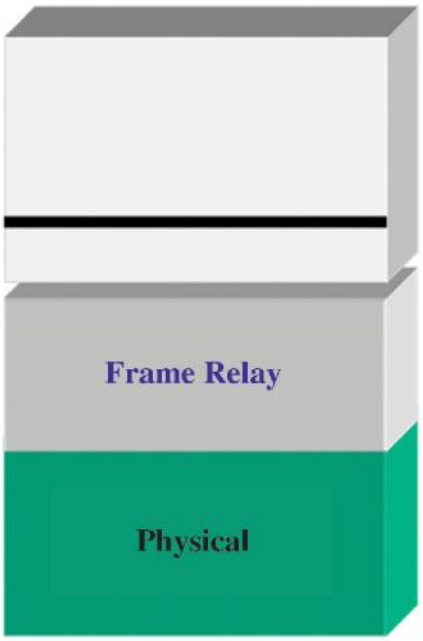

FIGURE 1.7

Frame relay used a reduced overhead at layer 2 of the OSI model.

data and had to find a lower-cost method to satisfy the data needs as well as faster networking speeds.

In 1992 both frame relay and ATM were introduced as means of moving away from the slower and more costly X.25 networks. With the implementation of frame relay the networks reduced overhead and allowed data to move at speeds of up to 2 Mbps and a streamlined layer 2 protocol. With reduced overhead and faster linkage frame relay spanned data rates of 56 kbps to 2 Mbps and reduced the error checking on the frames of information. Frame relay at the lower portion of layer 2 of the OSI model is shown in Figure 1.7.

Frame relay worked fine and still does, but the data needs were outstripping everything that frame relay could handle. As a result, a faster packet technique called Asynchronous Transfer Mode was developed to handle the speeds available on optical fiber networks. Speeds in ATM ranged from 50 to 622 Mbps, using a reduced overhead. Reducing the amount of error checking needs was an obvious fit for the telecommunications industry because fiber optics produced data at much higher throughput and lower errors. ATM then works at the bottom half of layer 2 of the OSI model similar to frame relay, as can be seen in Figure 1.8. The upper portion of layer 2 is called the ATM adaptation layer that is used to prepare the traffic based on the traffic type (circuit-switched voice, packet-switched voice or

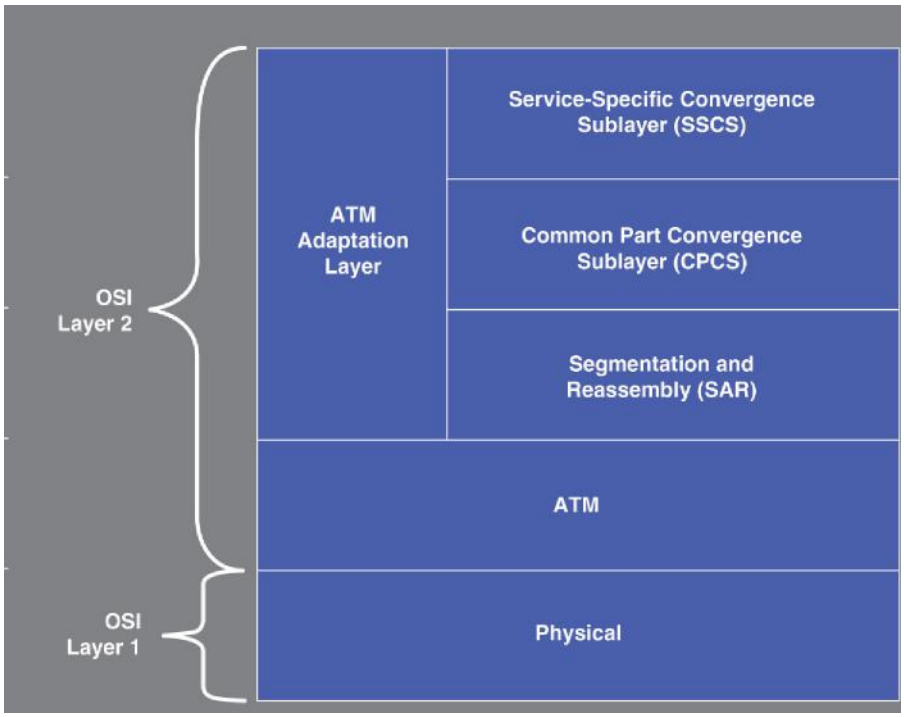

FIGURE 1.8

ATM operates at layer 2 of the OSI model.

video, packet-switched data, etc.). The figure shows that there are different steps to get the ATM cells ready for the network.

After all the work that was placed on the networks to ready the data for movement, what began as the IP (from the original ARPANET) became a better way to move data. In 1984 the TCP/IP stack version 4 (IPv4) was introduced as mentioned above as a means of DoD units to move data between disparate machines and protocols. This worked for many years and in 1995 the information highway of the future (as it was called) was brought about with the commercialization of the Internet. TCP is a smart protocol that was designed for reliable data transfer on an end-to-end basis, much like X.25 protocols were designed to carry the data reliably. TCP works at layer 4 of the OSI model.[3] IP is designed as a dumb protocol that guarantees nothing. IP does not guarantee delivery, is not concerned with proper sequencing (arrival) of the data, does not worry about error checking, and does not necessarily arrive on time. As a result, TCP is the protocol that handles these issues. One must remember that by this time the optical networks were delivering data (and voice) at higher,

[3]The DoD model had only four layers but comparisons are always drawn between TCP/IP and the OSI model. So for the purposes of explanation, the industry refers to TCP as a layer 4 OSI equivalent.

sample content of Securing VoIP: Keeping Your VoIP Network Safe

- read The Strangeness of Tragedy pdf, azw (kindle), epub, doc, mobi
- *download You Are What You Wear: What Your Clothes Reveal About You pdf, azw (kindle), epub*
- read online The Future of Warfare
- read online Immanuel Kant: Prolegomena to Any Future Metaphysics: That Will Be Able to Come Forward as Science: With Selections from the Critique of Pure Reason (Revised Edition) (Cambridge Texts in the History of Philosophy) here

- http://diy-chirol.com/lib/The-Strangeness-of-Tragedy.pdf
- http://fitnessfatale.com/freebooks/OLD-MAN--Perry-Rhodan-Silberb--nde--Band-33--M-87--Band-1-.pdf
- http://thewun.org/?library/The-Future-of-Warfare.pdf
- http://hasanetmekci.com/ebooks/Immanuel-Kant--Prolegomena-to-Any-Future-Metaphysics--That-Will-Be-Able-to-Come-Forward-as-Science--With-Selecti